REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested.

Claims 1-20 are pending. New claims 22-23 are added to secure an appropriate scope of protection to which applicants are believed entitled. Claim 21 has been cancelled without prejudice or disclaimer.

The objection to the specification as failing to provide antecedent basis for the claimed subject matter of claim 7 is not understood as the specification is believed to provide antecedent support at at least page 8, lines 7-9, page 13, lines 5-14, and page 22, lines 19-26. For at least this reason, the objection should be withdrawn.

The rejection of claims 12 and 19 under 35 U.S.C. 112, first paragraph, is believed overcome in view of the foregoing amendments and the rejection should be withdrawn.

The rejection of claim 18 under 35 U.S.C. 112, first paragraph, is hereby traversed as the instant specification at at least page 9, lines 27-29 describes the claimed, "selecting step can be based on the outcome of system calls including pass, failure, or both." The Examiner has failed to identify that the specification fails to teach how to make and use the claimed invention without undue experimentation, or that the scope of any enablement provided to one skilled in the art is not commensurate with the scope of protection sought by the claims. The Examiner has failed to specifically identify what information is missing and why one skilled in the art could not supply the information without undue experimentation. The Examiner is referred to MPEP §2164.05.

The Examiner has the initial burden of presenting by a preponderance of evidence why a person skilled in the art would not recognize in applicant's disclosure a description of the invention defined by the claims. The Examiner has failed to meet this burden. The Examiner has failed to provide reasons why persons skilled in the art would not have recognized that the inventor was in possession of the invention as claimed in view of the above noted disclosure.

Further still, it is believed that the disclosure reasonably conveys to a person of ordinary skill in the art that the inventor had possession at the time of filing of the claimed subject matter. There is a strong presumption that an adequate written description of the claimed invention is present when the application is filed. In re Wertheim, 541 F.2d 257, 263, 191 USPQ 90, 97 (CCPA 1976) ("we are of the opinion that the PTO has the initial burden of presenting evidence or reasons why persons skilled in the art would not recognize in the disclosure a description of the invention defined by the claims").

The Examiner is respectfully requested to provide findings identifying the claim limitations at issue and reasons why a person skilled in the art at the time the application was filed would not have recognized that the inventor was in possession of the invention as claimed in view of the above remarks and the instant specification. For at least this reason, the rejection should be withdrawn.

The rejection of claims 1, 17, and 18 under 35 U.S.C. 112, second paragraph, is believed overcome in view of the foregoing amendments and the rejection should be withdrawn.

The rejection of claims 1-21 under 35 U.S.C. 102(e) is hereby traversed as Crosbie et al. (U.S. 2002/0083343) fails to disclose all limitations of the present claimed invention. A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. Crosbie fails to disclose at least the step of "enabling the generation of audit data when a device driver is opened for read, and halting data generation when the device driver is closed."

The Examiner has failed to identify with specificity where Crosbie discloses enabling the generation of audit data when a device driver is opened for read and halting data generation when the device driver is closed. Paragraph 205 of Crosbie states that "a read() of /dev/idds [forces] the IDDS kernel driver 370 to read the next audit record block from the circular buffer." Thus, a read() causes the driver 370 to read the next audit record without specifying enabling the audit data generation and halting data generation based on the device driver opening/closing, respectively, as claimed. For at least this reason, the rejection of claim 1 should be withdrawn.

Claims 2-20 depend, either directly or indirectly, from claim 1, include further important limitations, and are patentable over Crosbie for at least the reasons advanced above with respect to claim 1. The rejection of claims 2-20 should be withdrawn.

With specific reference to claim 2, Crosbie fails to disclose storing related file information for each system call accessing files. Crosbie at paragraph 205 states that system call header related information is gathered. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 2 should be withdrawn.

With specific reference to claim 8, Crosbie fails to disclose setting selection masks based on system wide configuration related data structures for specifying data to be delivered as claimed in amended claim 8. Paragraph 761 of Crosbie states that trace and log message generation is controlled by setting of a command line argument. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 8 should be withdrawn.

With specific reference to claim 9, Crosbie fails to disclose formatting collected data into an audit record. Crosbie at paragraph 105 states that "[a] set of data gathering components . . . provides a way of observing what activity is occurring on the systems and networks" without disclosing the collecting data in a system call path and formatting the collected data into an audit record. The Examiner is requested to specifically identify where in the reference the Examiner believes the claimed limitation is to be found. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 9 should be withdrawn.

Similar to claim 9, with specific reference to claim 10, Crosbie fails to disclose that the collected data is a token stream. The Examiner is requested to specifically identify where in the reference the Examiner believes the claimed limitation is to be found. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 10 should be withdrawn.

With specific reference to claim 13, Crosbie fails to disclose a selecting step for selecting which data to collect before the collecting step. The Examiner is requested to identify with specificity where in paragraph 205 of the reference, the Examiner believes the selecting step is disclosed. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 13 should be withdrawn.

With specific reference to claim 14, Crosbie fails to disclose that the selecting step is based on process, user, group, filename information and/or time intervals. The Examiner is

requested to identify with specificity where in paragraph 205 of the reference, the Examiner believes the selecting step based on process, user, group, filename information and/or time intervals is disclosed. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 14 should be withdrawn.

With specific reference to claim 18, Crosbie fails to disclose a selecting step based on an outcome of system calls including pass, failure, or both. The Examiner is requested to identify with specificity where in paragraph 205 of the reference, the Examiner believes the selecting step based on process, user, group, filename information and/or time intervals is disclosed. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 18 should be withdrawn.

Further, new claim 22 is patentable over Crosbie as Crosbie fails to disclose at least a selecting step which is based on an outcome of system calls including pass, failure, or both. Contrary to the Examiner's assertion regarding claim 18 (hereby incorporated into claim 22), paragraph 205 of Crosbie fails to disclose a selecting step for selecting which data to collect before the collecting step. The Examiner is requested to identify with specificity where in paragraph 205 of the reference, the Examiner believes the selecting step (and selecting step based on the outcome of system calls including pass, failure, or both) is disclosed. Because the claimed limitation of at least selecting which data to collect before the collecting step is not found in Crosbie, claim 22 is believed to be patentable over Crosbie.

New claim 23 recites a method of generating kernel audit data comprising: storing system call parameters or data the parameters point to at the beginning of a system call; and triggering data delivery at the end of the system call and generating an audit record and depositing the audit record in a circular buffer if, based on the success or failure of the system call, auditing of the system call should continue as specified in a post-call selection flag. The method of new claim 23 is not disclosed by Crosbie and is patentable over Crosbie.

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN & BERNER, LLP

Randy A. Noranbrock

Randy A. Noranbrock
Registration No. 42,940

Customer Number: 22429
1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: December 22, 2005
KMB/RAN/iyr